



**TWRS-P PROJECT
SAFETY REQUIREMENTS DOCUMENT
ABAR-W375-99-00015, Rev. 1**

CONTENTS

1.0 INTRODUCTION.....	A-1
2.0 PROCESS INITIATION.....	A-1
3.0 IDENTIFICATION OF WORK.....	A-1 a
4.0 HAZARD EVALUATION.....	A-2
4.1 IDENTIFICATION OF HAZARDS.....	A-3
4.2 IDENTIFICATION OF POTENTIAL ACCIDENT/EVENT SEQUENCES.....	A-3
4.3 ESTIMATION OF CONSEQUENCES.....	A-4
4.3.1 Accident Severity Level Identification.....	A-4
4.3.2 Accident Analysis	A-5
4.3.3 Normal Conditions.....	A-6
4.4 ESTIMATION OF ACCIDENT FREQUENCIES	A-6
4.5 CONSIDERATION OF COMMON CAUSE/COMMON MODE FAILURES.....	A-6
4.6 DEFINITION OF DESIGN BASIS EVENTS.....	A-7
4.7 DEFINITION OF OPERATING ENVIRONMENT	A-7
4.8 IDENTIFICATION OF POTENTIAL CONTROLS.....	A-7
4.9 DOCUMENTATION.....	A-8
5.0 DEVELOPMENT OF CONTROL STRATEGIES.....	A-8
6.0 CLASSIFICATION OF STRUCTURES, SYSTEMS, AND COMPONENTS.....	A-12
7.0 IDENTIFICATION OF STANDARDS.....	A-12 Cb
8.0 CONFIRMATION OF STANDARDS.....	A-15
9.0 FORMAL DOCUMENTATION.....	A-15
10.0 RECOMMENDATION	A-15
11.0 DEFINITIONS.....	A-15

A



**TWRS-P PROJECT
SAFETY REQUIREMENTS DOCUMENT
ABAR-W375-99-00015, Rev. 1**

This page intentionally left blank.



**TWRS-P PROJECT
SAFETY REQUIREMENTS DOCUMENT
ABAR-W375-99-00015, Rev. 1**

1.0 INTRODUCTION

This standard implements the process for establishing a set of radiological, nuclear, and process safety requirements and standards as described in DOE/RL-96-0004 and RL/REG-98-17. BNFL Inc. refers to this process as Integrated Safety Management (ISM).

The activities described below establish radiological, nuclear and process safety standards and requirements for design, construction and operation of the facility. Establishment of safety standards and requirements is an iterative process that takes place throughout the life of the project. As the design evolves, the process repeatedly evaluates these standards and requirements based on the evolving design.

The Safety Requirements Document (SRD) provides formal documentation of the standards, which are a results of this process. The SRD is updated as required to reflect the results of successive iterations of the standards and requirements ~~and~~-identification process (i.e., the ISM process).

2.0 PROCESS INITIATION

The TWRS-P Project Manager shall ensure implementation of the Project Management Plan, thus assuring that adequate resources with appropriate technical background are available and organized to perform subsequent tasks. This activity also assures that the input information required for the safety standards and requirements identification process has been collected and organized. This input information includes the top-level safety standards and principles stipulated by DOE in DOE/RL-96-0006 and the laws and regulations applicable to the TWRS Privatization project.

The DOE/RL-96-0004 safety requirements and standards identification ~~P~~rocess ~~M~~anager for the ~~TWRS-P~~ project is the ~~Safety and Regulatory Programs~~ Manager, Radiological, Nuclear, and Process Safety.

The Process Manager chairs the DOE/RL-96-0004 safety requirements and standards identification ~~P~~rocess ~~M~~anagement ~~T~~eam (PMT)~~shall be. The PMT is constituted in accordance with project implementing documents~~~~consist of the following TWRS-P personnel and includes managers from the following project organizations :~~

- Environmental, Safety, & Health~~Safety and Regulatory Programs Manager~~
 - Functional Engineering~~Safety Process Manager~~
 - Operations~~Design Safety Implementation Manager~~
 - Area Project Design~~HLW and LAW Vitrification Project Design Managers~~
- ~~—BOF and Pretreatment Project Design Managers.~~



**TWRS-P PROJECT
SAFETY REQUIREMENTS DOCUMENT
ABAR-W375-99-00015, Rev. 1**

The Process Management Team (PMT) shall oversee the ISM process and shall provide resources and resolve issues as necessary. The PMT shall set up Integrated Teams for the conduct of ISM on a plant system basis. Individual PMT members shall provide various subject matter experts to help fulfill the roles required of the Integrated Teams for conduct of the ISM process.

3.0 IDENTIFICATION OF WORK

The aim of this activity is to describe the work that will be performed so that the hazards inherent in the work can be identified and evaluated. Work activity experts who have extensive knowledge of the overall processing approach and are integrally associated with the facility



**TWRS-P PROJECT
SAFETY REQUIREMENTS DOCUMENT
ABAR-W375-99-00015, Rev. 1**

design shall perform this activity. Work Activity Experts shall be drawn from the following TWRS-P organizations:

~~—Functional staff of the TWRS-P Engineering Manager~~

- Technical staff of the ~~HLW and LAW Vitrification~~applicable Project Design Manager(s)

~~—Technical staff of the BOF and Pretreatment Project Design Managers~~

- Operations staff.

When appropriate, the Process Management Team may also draw Work Activity Experts from the staff of the Functional Engineering Manager.

~~The process management team shall oversee the Identification of Work Activity and provide additional technical resources as necessary.~~

In an overall sense, identification of work involves definition of the project mission and identification of the processes that must be performed to accomplish the mission. It includes selection of optimum functions, processes, and parameters through trade studies and definition of functional requirements. Identification of work for the purpose of design development involves definition of various plant systems, structures, and components. This latter definition is the focus for the Integrated Teams created to conduct ISM on a plant system basis.

The product of this activity includes:

- Process description
- System descriptions
- Descriptions of key structures
- Basis of design documents
- PFDs, MFDs, and P&IDs

The results of the identification of work activity shall be documented in the SRD by inclusion or by reference.

The identification of work activity is an iterative process. Identification of work will be reconsidered in light of design evolution, the outcome of hazard evaluations, and the development of hazard control strategies.

4.0 HAZARD EVALUATION

The aim of the hazard evaluation activity is to identify and characterize the hazards resulting from the work. ~~A hazard evaluation~~The Integrated Teams shall conduct the hazard evaluation activity. ~~This on a plant system basis. These~~ teams shall include work activity experts, hazard assessment experts, and hazard control experts.



**TWRS-P PROJECT
SAFETY REQUIREMENTS DOCUMENT
ABAR-W375-99-00015, Rev. 1**

Work Activity Experts shall be drawn from the following TWRS-P organizations:

~~Functional staff of the TWRS-P Engineering Manager~~

- Technical staff of the ~~HLW and LAW Vitrification~~applicable Project Design Manager(s)

~~Technical staff of the BOF and Pretreatment Project Design Manager~~

- Operations staff.

When appropriate, the Process Management Team may also draw Work Activity Experts from the staff of the Functional Engineering Manager.

Hazard assessment experts and hazard control experts shall generally be members of the technical staffs of the Design Safety Implementation Manager and of the Safety Process Manager. The process management team shall provide additional technical resources as required to evaluate the hazards.

~~The Process Management Team shall oversee the hazard evaluation activity and resolve issues raised by the hazard evaluation team.~~

The hazard evaluation shall address hazards inherent in normal operation as well as potential accidents resulting from abnormal internal and external events.

The hazard evaluation shall comprise the following elements:

- Identification of Hazards
- Identification of Potential Accident/Event Sequences
- Estimation of Accident Consequences
- Estimation of Accident Frequencies
- Consideration of Common Cause and Common Mode Failures
- Definition of Design Basis Events
- Definition of Operating Environment
- Identification of Potential Control Strategies
- Documentation

These elements are discussed below.

4.1 IDENTIFICATION OF HAZARDS

The objective of this element is to systematically identify the hazards associated with the defined work.

The ~~hazard evaluation team~~[Integrated Teams](#) shall compile a list of hazardous materials and energy sources associated with the facility processes, design and operations. This list shall be compiled based on the identified work. This compilation provides information used to identify potential accidents resulting in the uncontrolled release of hazardous material or energy to workers, the public and the environment. The team may use checklists to guide the compilation process and to assure that all potential hazards from both natural and manmade sources originating from outside and inside the facility are addressed.

4.2 IDENTIFICATION OF POTENTIAL ACCIDENT/EVENT SEQUENCES

The objective of this element is to perform a structured and systematic examination of the facility and its operations to identify potential accidents (including common mode and common cause failures). The team shall conduct this examination using methodologies and guidelines in AIChE (1992).

4.3 ESTIMATION OF CONSEQUENCES

4.3.1 Accident Severity Level Identification

A severity level, SL, shall be assigned to each postulated radiological accident. The severity level shall reflect the unmitigated consequences of the postulated accident. Unmitigated consequences shall account for the quantity, form and location of the radioactive material available for release, and the energy sources available to interact with the hazardous material. Unmitigated consequences shall not account SSCs that serve to prevent or mitigate the release. Specifically, unmitigated consequences shall be evaluated on the basis of a ground level release. The severity level shall be defined as follows:

SL	Facility Worker Consequence	Co-Located Worker Consequence	Public Consequence
SL-1	> 25 rem/event	> 25 rem/event	> 5 rem/event
SL-2	5 - 25 rem/event	5 - 25 rem/event	1 - 5 rem/event
SL-3	1 - 5 rem/event	1 - 5 rem/event	0.1 – 1 rem/event
SL-4	< 1 rem/event	< 1 rem/event	< 0.1 rem/event

These severity levels are related to the radiological and process standards of SRD [Section Chapter 2.0](#) as follows:

- The unmitigated consequences associated with SL-1 events exceed the radiological standards for extremely unlikely events (SRD Safety Criterion 2.0-1).
- The unmitigated consequences associated with SL-2 events are below the radiological standards for extremely unlikely events (SRD Safety Criterion 2.0-1).
- The unmitigated consequences associated with SL-3 events are below the radiological standards for unlikely events (SRD Safety Criterion 2.0-1).
- The unmitigated consequences associated with SL-4 events are below the radiological standards for anticipated events (SRD Safety Criterion 2.0-1).

Consequences to the facility worker shall be evaluated at the worst-case occupied location. Consequences to the co-located worker and the public shall be evaluated at the locations specified in Appendix D to the *Safety Requirements Document, Volume II*.

Early in the design, the severity level is estimated based on the experience of the ~~hazard evaluation team~~[Integrated Teams](#). As the design progresses, these estimates are confirmed through the formal accident analyses described in Section 4.3.2. These accident analyses do not address all of the potential accidents identified, but they do address bounding examples of each type of accident. The team should use the results of the accident analyses to validate the severity level estimates for potential accidents not addressed in the formal accident analyses.

The potential consequences of releases of hazardous chemicals shall also be assessed. These hazards shall be subject to the graded application of the Process Safety Management (PSM) rule. If the type and quantity of chemical involved could result in concentrations equivalent to ERPG-2, for example, the full extent of the PSM rule shall be applicable.

4.3.2 Accident Analysis

Accident analyses provide confirmation that the design satisfies the radiological and process standards in the SRD. Accident analyses also provide confirmation of the severity levels assigned to potential accidents.

The formal accident analyses shall address design basis external events and natural phenomena as well as postulated internal events.

The postulated internal events shall be grouped by type. Accident types applicable to the TWRS-P include the following:

- Liquid spills
- Spills of solid materials
- Pressurized releases
- Chemical reactions
- Boiling
- Flammable gas ignition (e.g., hydrogen in air)
- Fires
- Load drops
- Radiation exposure
- Criticality

As a minimum, the accident analysis shall address the most severe credible event of each type.

Initially, the accident analysis shall evaluate the unmitigated consequences of the postulated accidents. As control strategies are developed, the accident analysis shall also evaluate the impact of the SSCs that implement the control strategy on the potential consequences.

The accident analysis shall consider the following factors:

- Inventory of material at risk in the scenario.
- The respirable release fraction for the accident scenario. This is a function of the composition of the material at risk, of the form of the material, and of the interaction between the material at risk and the energy available in the accident scenario.
- The fraction of the airborne material released to potentially occupied locations or the environment.

- Bounding atmospheric dispersion coefficients (if appropriate).
- Radiological composition of the material released.
- External radiation field.
- Exposure times.

The accident analysis shall address the potential consequence to facility workers, co-located workers, and the public.

4.3.3 Normal Conditions

Some hazards inherent in normal operation must be mitigated to comply with the standards for normal operation in SRD ~~Section~~ [Chapter](#) 2.0. Such hazards shall be addressed in accordance with the TWRS-P Radiation Protection Plan.

4.4 ESTIMATION OF ACCIDENT FREQUENCIES

There is normally insufficient information early in the design to accurately quantify the frequency of postulated internal events because this frequency depends on the design of the SSCs that implement the control strategy used to manage the hazard. At ~~this~~ [an](#) early stage, frequency evaluations may be based on the [team's](#) experience ~~of the hazard evaluation team~~ with similar hazards in similar facilities. The team shall validate these estimates as the design develops.

As the design matures, information on the frequency of hazardous events is gained from the use of hazard evaluation techniques that provide frequency data (i.e., HAZOP, FMEA, Event Trees, and Fault Trees). Evaluations of the frequency of failure in redundant systems or in diverse systems using similar equipment shall consider dependent failures.

The frequencies of design basis external events may be derived from existing analyses (e.g., safety analyses for adjacent facilities), from evaluation of historical data (e.g., transportation data), or from site-specific information (e.g., seismic history).

4.5 CONSIDERATION OF COMMON CAUSE/COMMON MODE FAILURES

The following are typical common cause events:

- Natural phenomena events
- External man made events
- Loss of electrical power
- Fire
- Internal missiles
- Internal flooding

Common cause events should be treated as discrete events in the hazard analysis. The analyses of common cause events shall focus on identifying provisions to prevent the loss of safety function. The analyses of natural phenomena events shall consider induced effects, such as fire and loss of electrical power.

Common mode failures shall be addressed through dependent failure modeling as required by Section 4.4 above.

4.6 DEFINITION OF DESIGN BASIS EVENTS

The hazard evaluation shall identify a set of internal design basis events. These events shall be selected to define a set of bounding performance requirements for the SSCs relied upon to control the hazards.

The hazard evaluation shall define a set of external man made design basis events. These events shall be selected based on the results of the hazard analysis to define a set of bounding performance requirements for the SSCs relied upon to mitigate these events.

[The Integrated Teams perform the identification of internal and external design basis events.](#)

Design basis natural phenomena shall be as defined in ~~the SRD Sections~~ [Safety Criteria](#) 4.1-3 and 4.1-4.

4.7 DEFINITION OF OPERATING ENVIRONMENT

The hazard evaluation shall define a set of bounding operating conditions in which SSCs relied upon to control hazards must function. Environmental parameters to be addressed include the following:

- Temperature
- Pressure
- Humidity
- Radiation Levels
- Chemical Environment

4.8 IDENTIFICATION OF POTENTIAL CONTROLS

Based on the experience and judgement of team members, the ~~hazard evaluation~~integrated team shall identify an initial set of potential hazard controls to manage each potential accident. This set of potential hazard controls shall address means of preventing the potential accident and should address means of mitigating the consequences of the accident. The function(s) of each potential hazard control should be clearly described. Potential hazard controls shall be identified to manage accident conditions arising from upsets in the process, conditions arising from external events, and conditions inherent in the normal operation of the process.

4.9 DOCUMENTATION

The hazard evaluation shall be documented in a hazard analysis report (HAR). The results of the hazard evaluation shall be contained in a hazard database. For each hazard considered, the hazard database shall record the following information produced by the hazard evaluation:

- Hazard identifier
- Hazard description
- Initiators
- Hazard severity level estimate (based on unmitigated consequences)
- Severity level basis
- Assumptions affecting the release (material at risk, energy available, etc)
- Hazard frequency estimate
- Basis for frequency estimate
- Potential controls and functions
- References for the hazard (these would typically be products of the work identification process)

Hazard evaluation documentation shall be included in the SRD by inclusion or by reference. This documentation shall include the following:

- Description of the comprehensive approach to hazard evaluation
- Description of the methodology for identification and quantification of work hazards
- Description of the methodology for identifying potential accident scenarios
- Description of the methodology for consequence assessment
- Clear identification of assumptions (e.g., quantity and form of material at risk, rate of release and relevant process conditions) that may drive or inhibit the potential accident must be clearly identified
- Description of results
- Evidence of appropriate staffing, and adequate technical staffing and structure applied to the hazard evaluation

5.0 DEVELOPMENT OF CONTROL STRATEGIES

The aim of the development of control strategies activity is to identify a means of controlling each of the hazards identified in the hazard evaluation. ~~A~~ The Integrated ~~t~~ Teams of work activity experts, hazard assessment experts and hazard control experts performs this activity.

Work activity experts shall be drawn from the following TWRS-P organizations:

~~—Functional staff of the TWRS-P Engineering Manager~~

- Technical staff of the ~~HLW and LAW Vitrification~~applicable Project Design Manager(s)

~~—Technical staff of the BOF and Pretreatment Project Design Manager~~

- Operations staff.

When appropriate, the Process Management Team may also draw Work Activity Experts from the staff of the Functional Engineering Manager.

Hazard assessment experts and hazard control experts shall generally be members of the technical staffs of the Design Safety Implementation Manager and of the Safety Process Manager. The process management team members shall provide additional technical resources as required to develop the control strategies.

~~The process management team shall oversee the development of control strategies activity and resolve issues raised by the control strategy development team.~~

The ~~control strategy development team~~Integrated Teams selects ~~a~~ preferred control strategies ies based on the set of potential controls identified by the hazard evaluation team. Selection of the preferred strategy considers the following factors:

- The functions required of the strategy in order to control the hazard
- The degree of defense in depth and reliability provided by the control strategy. The Implementing Standard for Defense in Depth provides guidance in this area.
- Applicable design basis events
- The operating environment in which the SSCs implementing the control strategy must function
- Effectiveness and efficiency of the control strategy
- Conformance with the DOE stipulated top level standards
- Compliance with applicable laws and regulations

The control strategy will typically comprise a series of elements including some or all of the following:

- Passive and/or active SSCs that function to prevent the release (that is, SSCs that reduce the probability that a release will occur)
- Passive and/or active SSCs that function to mitigate the release (that is, SSCs that reduce the consequences once a release has occurred)

- Administrative controls (for example, limits on inventory).

Consistent with the defense in depth principle, the control strategy development should emphasize preventive measures. It should also emphasize passive SSCs over active SSCs and retention of released material over dispersion. Ideally, the preferred control strategy should incorporate SSCs that prevent releases and SSCs that mitigate the consequences of a release, should it occur.

Once the preferred control strategy is identified, it shall be evaluated using the techniques described in Section 4.3 through 4.5. In addition, the evaluation of the control strategy shall identify the measures necessary to assure that it performs its functions reliably. Such measures include maintenance requirements, testing intervals and calibration frequency. The results of this evaluation serve to confirm that the control strategy is capable of satisfying SRD Safety Criteria 2.0-1.

If credit is taken for operator action to satisfy the public radiological exposure standards of Safety Criterion 2.0-1, adequate radiation protection is provided to permit access and occupancy of the control room or other control locations under accident conditions without personnel receiving radiation doses in excess of 5 rem TEDE whole body gamma and 30 rem beta skin for the duration of the accident. If credit is taken for operator action to satisfy public chemical exposure to EPRG-2 limits, provisions for operational access and control are made so that the operator exposure does not exceed the EPRG-2 limits.

Documentation of the hazard control strategy development process shall clearly indicate selection of the control strategies and show the linkage of the control strategies to the respective hazards. ~~be a narrative defining the overall approach to control a specific pre-identified hazard.~~ The control strategy should be described in terms of the safety functions required (e.g., limit release of radionuclides, etc.) and in terms of a set of engineered features, administrative controls (procedures and training), and management systems selected for implementing the strategy. When the nature of the hazard is such that the appropriate control strategy is self-evident, the documentation need only demonstrate that the control strategy meets most, if not all, of the selection criteria and need not provide a discussion of other, nonapplicable control strategies. Similarly, where a proven control strategy that is appropriate to the hazard exists and it is obvious to the team that there are no other alternative control strategies that could be equally attractive, then the documentation need only demonstrate that the control strategy meets most, if not all, of the selection criteria. Otherwise, the documentation should identify all control strategies considered and provide a defensible rationale for selection of the preferred strategy.

The following information produced by the control strategy definition shall be recorded in the hazard database:

- Preferred control strategy
- [Linkage of the control strategy to the respective hazards](#)
- Rationale for preferred control strategy selection
- Defense in depth provided
- Control strategy functions and performance requirements
- Estimate of the unmitigated event frequency
- Estimate of the consequences from the mitigated event
- Estimate of the mitigated event frequency
- Applicable design basis events (e.g., design basis earthquake)

~~This information in the hazard database links the specific hazards to specific control strategies.~~

One of the issues in developing a control strategy for a particular hazard is determining the number of layers of prevention and mitigation appropriate for the hazard. The control strategies shall conform to the requirements defined in the Implementing Standard for Defense in Depth. In addition, the following guidance shall be considered in developing control strategies.

The general TWRS-P design approach is to provide two confinement barriers against the release of hazardous materials. The process vessels and piping form the primary confinement barrier;

the process cells and associated ventilation system form the secondary confinement barrier. Releases from the primary confinement are mitigated by the secondary confinement.

The accident severity levels defined in Section 4.3.1 are related to the exposure standards in SRD Safety Criterion 2.0-1. The SRD Safety Criterion 2.0-1 exposure standards are frequency based, so it is possible to establish target frequencies for events with a given severity level. The target frequencies tabulated below are consistent with SRD Safety Criterion 2.0-1.

SL	Event Target Frequency (yr⁻¹)
SL-1	$<10^{-6}$
SL-2	$<10^{-4}$
SL-3	$<10^{-2}$
SL-4	$<10^{-1}$

These target frequencies may be used to guide control strategy development as described below. For SL-1 events:

- Meeting the target frequency will usually require a control strategy that incorporates diverse and independent SSCs that act to prevent and mitigate the event.
- Meeting the target frequency will usually require diverse SSCs that act to prevent the release.
- The degree of mitigation required depends on the release frequency, that is, on the reliability of the preventive SSCs. For example, assume that the preventive SSCs assure that the frequency of release is less than 10^{-4} per year, but more than 10^{-6} per year. This frequency is not acceptable for events that have SL-1 level consequences, but is acceptable for events that have SL-2 level consequences. Therefore, the control strategy would need to provide enough mitigation to reduce the consequences of the release to the levels associated with a SL-2 event, as a minimum. The combined reliability of the preventive SSCs and the SSCs that provide mitigation needs to satisfy the target frequency for a SL-1 event. That is, the probability that the SSCs that provide mitigation will fail should be on the order of 10^{-2} , given the release.
- SSCs in control strategies for SL-1 events shall satisfy the single failure criteria in the Implementing Standard for Defense in Depth.

For SL-2 events:

- Meeting the target frequency will usually require a control strategy that incorporates diverse and independent SSCs that act to prevent and mitigate the event.

- The degree of mitigation required depends on the release frequency, that is, on the reliability of the preventive SSCs. For example, assume that the only viable preventive SSCs assure that the frequency of release is less than 10^{-2} per year, but more than 10^{-4} per year. This frequency is not acceptable for events that have SL-2 level consequences, but is acceptable for events that have SL-3 level consequences. Therefore, the control strategy would need to provide enough mitigation to reduce the consequences of the release to the levels associated with a SL-3 event, as a minimum. The combined reliability of the preventive SSCs and the SSCs that provide mitigation needs to satisfy the target frequency for a SL-2 event. That is, the probability that the SSCs that provide mitigation will fail should be on the order of 10^{-2} , given the release.
- SSCs in control strategies for SL-2 events should satisfy the single failure criteria in the Implementing Standard for Defense in Depth.

For SL-3 and SL-4 events:

- The mitigation provided by the secondary confinement would be adequate to satisfy SRD Safety Criterion 2.0-1. It would also be adequate to satisfy SRD Safety Criteria 1.0-3 through 1.0-5. However, preventive features should be considered consistent with the defense in depth principle.
- A single preventive SSC may satisfy the frequency goal for SL-3 and SL-4 events.
- SSCs in control strategies for SL-3 and SL-4 events need not satisfy the single failure criteria in the Implementing Standard for Defense in Depth.

6.0 CLASSIFICATION OF STRUCTURES, SYSTEMS, AND COMPONENTS

The design classification process used on the TWRS-P Project provides a consistent, project-wide approach for the classification of the TWRS-P Facility SSCs based on their importance to controlling normal releases and accident prevention and mitigation. This approach ensures that SSCs are designed, constructed, fabricated, installed, tested, operated, and maintained to quality standards commensurate with the importance of the functions that need to be performed. As the facility moves to deactivation, and the safety functions change, the classification of SSCs can be revised as necessary.

BNFL Inc. has established a design classification system to provide assurance to DOE that the defined safety functions of SSCs will perform as intended.

SSCs defined as Important-to-Safety for the TWRS-P Facility include the following:-

- 1) SSCs needed to prevent or mitigate accidents that could exceed public or worker radiological and chemical exposure standards of Safety Criteria 2.0-1 and 2.0-2 and SSCs needed to prevent criticality. This set of SSCs includes both the front line and support systems needed to meet these exposure standards or to prevent criticality. This set of Important-to-Safety SSCs ~~are~~ is designated as Safety Design Class, as defined by SRD Safety Criterion 1.0-8.
- 2) SSCs needed to achieve compliance with the radiological or chemical exposure standards for the public and workers during normal operation; and SSCs that place frequent demands on, or adversely affect the function of, Safety Design Class SSCs if they fail or malfunction. This set of Important-to-Safety SSCs ~~are~~ is designated as Safety Design Significant, as defined by SRD Safety Criterion 1.0-8.

The processes for identifying the SSCs for each of the two groups of SSCs Important-to-Safety and the requirements assigned to each of the two groups are discussed below.

Safety Design Class SSCs typically are identified by the results of accident analyses that show the potential for exposure standards to be exceeded or prevent a criticality. However, additional items may also be designated Safety Design Class independent of a specific accident analysis. These are items that protect the facility worker from potentially serious events. Typically, these events are deemed to present a challenge to the facility worker severe enough that mitigation is prudent, without the need to perform a specific consequence analysis.

Safety Design Significant SSCs are identified in several ways including: (1) SSCs identified as significant contributors to safety by the analyses that confirm the facility accident risk goals are met (this is one way to identify SSCs that place frequent demands on, or adversely affect the function of, Safety Design Class SSCs if they fail or malfunction), (2) SSCs that are needed to ensure that standards for normal operation are not exceeded (e.g., bulk shield walls or radiation monitors), (3) SSCs selected based on the dictates of nuclear and chemical facility experience and prudent engineering practices, and (4) SSCs whose failure could prevent Safety Design Class SSCs from performing their safety function (e.g., Seismic II/I items).

When an SSC is designated as Safety Design Class it has the following attributes:

- 1) Quality Level 1 (QL-1) is applied to the SSC to provide added assurance that the SSCs can perform their specified safety function.
- 2) For an active system or component, the safety function is preserved by application of defense-in-depth such that failure of the system or component will not result in exceeding a public or worker accident exposure standard. For a mitigating feature, this means that, given that the accident has occurred, the consequence of the accident will not result in exceeding a public or worker exposure standard. For a preventative feature, this means that the failure of

the system or component will not allow the accident to occur and progress such that a public or worker accident exposure standard is exceeded. If the hazard analysis shows that these requirements are necessary, this requirement may be achieved by designing the Safety Design Class system or component to withstand a single active failure or by designating two separate and independent systems or components as Safety Design Class.

- 3) The SSC is designed to withstand the effects of natural phenomena such that it can perform any safety functions required as a result of a natural phenomena event in accordance with Safety Criterion 4.1-3.
- 4) General design requirements are applied as identified in ~~Section~~ [Chapter](#) 4.0 of the SRD for Safety Design Class SSCs.
- 5) Specific design requirements based on the type of component are applied as invoked in SRD Chapter 4.0.
- 6) Other design requirements may be applied based on the specific safety function to be performed by the Safety Design Class SSC. This specific safety function is determined from the accident analysis that identified the need for prevention or mitigation by Safety Design Class SSCs.
- 7) Operational requirements (e.g., periodic testing and preventative maintenance) are applied to Safety Design Class SSCs through the application of Technical Safety Requirements.

When an SSC is classified as Safety Design Significant it has the following attributes.

- 1) Quality Level 2 (QL-2) is applied to the SSC to provide added assurance that the SSCs can perform their specified safety function.
- 2) The SSC is designed to withstand the effects of natural phenomena such that it can perform its safety functions required as a result of a natural phenomena event in accordance with Safety Criterion 4.1-4.
- 3) General and specific design requirements are applied as identified in ~~Section~~ [Chapter](#) 4.0 of the SRD for Safety Design Significant SSCs.
- 4) Other design requirements again may be applied based on the specific safety function to be performed by the Safety Design Significant SSC.

7.0 IDENTIFICATION OF STANDARDS

Identification of standards is an iterative activity. Initially, the set of standards and requirements is derived from a general understanding of the hazards inherent in the work. As the design



**TWRS-P PROJECT
SAFETY REQUIREMENTS DOCUMENT
ABAR-W375-99-00015, Rev. 1**

evolves, the hazard evaluation and the development of the control strategies justify tailoring the set of standards to better fit the hazards.

The ~~standards~~-identification ~~activity~~ of engineering/design, manufacture/fabrication, and construction standards is performed by an integrated team including work activity experts, hazard assessment experts, hazard control experts, and ESH standards experts. Identification of other standards (e.g., quality assurance, conduct of operations, etc.) will be performed by specially constituted teams formed by the PMT. The aim of this activity is to identify a tailored set of standards and requirements that will assure adequate safety when implemented.

Work activity experts shall be drawn from the following TWRS-P organizations:

~~—Functional staff of the TWRS-P Engineering Manager~~

- Technical staff of the ~~HLW and LAW Vitrification~~applicable Project Design Manager(s)

~~—Technical staff of the BOF and Pretreatment Project Design Manager~~

When appropriate, the Process Management Team may also draw Work Activity Experts from the staff of the Functional Engineering Manager.

Hazard assessment experts and hazard control experts shall generally be members of the technical staffs of the Design Safety Implementation Manager and of the Safety Process Manager. The process management team shall provide additional technical resources as required to identify the standards.

ESH standards experts shall be drawn from the following TWRS-P organizations:

- ~~Functional~~s Staff of the TWRS-P ~~Functional~~ Engineering Manager
- Technical staff of the ~~HLW and LAW Vitrification~~ Project Design Managers
- ~~Technical staff of the BOF and Pretreatment Project Design Manager~~
- Technical staff of the Safety and Regulatory Programs Manager

~~The process management team shall oversee the identification of standards activity and resolve issues raised by the standards identification team.~~

The standards identified are evaluated and tailored for each control strategy based on compliance with applicable laws and regulations and conformance with the DOE-stipulated top level standards, plus the output of the preceding hazard evaluation and control strategy development steps. Typical considerations include the following:

- the severity level of the hazard
- the number of independent SSCs that comprise the control strategy
- the control strategy functions – recognizing that a specific control strategy may have multiple functions and serve to control multiple hazards
- the service environment
- the applicable design basis events

- the target reliability for the control strategy.

The target frequencies described in Section 4 provide a basis for establishing target reliabilities for the SSCs that comprise the control strategy. The combined reliability of the preventive SSCs and the SSCs that provide mitigation must be consistent with the target frequency for the unmitigated event. The reliability of the preventive SSCs should be consistent with the release frequency used to determine the degree of mitigation provided.

Documentation of the standards and requirements identification process provides justification of the set selected and links each control strategy to its associated set of standards. The information generated during standards selection is retained in database form for each control strategy:

- Control strategy
- Service environment
- Applicable design basis events
- Applicable standards
- Performance requirements
- Testing/calibration requirements
- In-service inspection requirements
- Maintenance requirements
- Quality level
- Standards justification

This information is structured so it can be linked to the control strategies in the hazard schedule. This provides a link from the hazards through the control strategies to the standards. Not all of this information will be available early in the design. For example, it will not be possible to define maintenance and testing requirements until the design is mature.

The standards identified through this activity shall be reflected in the SRD.

As the standards are tailored, discrepancies with the current version of the SRD may arise. Such discrepancies shall be recorded. Formal changes to the SRD require approval from the Regulatory Unit.

8.0 CONFIRMATION OF STANDARDS

Based on the recommendation of the ~~P~~rocess ~~M~~anager, the TWRS-P Project Manager requests the Project Safety Committee (PSC) to confirm the selected set of standards. The PSC defines a review approach, carries out the review, and documents the findings of the review. Comments by the PSC shall receive formal disposition by the Process Management Team.

9.0 FORMAL DOCUMENTATION

Following confirmation by the PSC, the results of the standards selection process ~~shall be described in the Integrated Safety Management Plan. The results of the process~~ shall be documented in the Safety Requirements Document (SRD). The SRD shall incorporate documentation supporting these results by reference. The SRD shall identify and justify the set of requirements and standards selected to provide adequate protection of workers, the public, and the environment.

10.0 RECOMMENDATION

~~The TWRS P Manager of Operations certifies that the recommended set of standards, w~~The recommended set of standards shall be certified in accordance with project implementing documents. When properly implemented, the set of standards:

- 1) Provides adequate safety
- 2) Complies with applicable laws and regulations
- 3) Conforms with the Top-Level Safety Standards and Principles.

11.0 DEFINITIONS

Credible event: Any event with a frequency greater than 10^{-6} per year, including allowance for uncertainties.

Important to Safety: Structures, systems, and components that serve to provide reasonable assurance that the facility can be operated without undue risk to the health and safety of the workers and the public. It encompasses the broad class of facility features addressed (not necessarily explicitly) in the top-level radiological, nuclear, and process safety standards and principles that contribute to the safe operation and protection of workers and the public during all phases and aspects of facility operations (i.e., normal operation as well as accident mitigation).

This definition includes not only those structures, systems, and components that perform safety functions and traditionally have been classified as safety class, safety-related, or safety-grade, but also those that place frequent demands on or adversely affect the performance of safety functions if they fail or malfunction, i.e., support systems, subsystems, or components. Thus, these latter structures, systems, and components would be subject to applicable top-level radiological, nuclear, and process safety standards and principles to a degree commensurate with their contribution to risk. In applying this definition, it is recognized that during the early stages of the design effort all significant systems interactions may not be identified and only the traditional interpretation of important to safety, i.e., safety-related, may be practical. However, as the design matures and results from risk assessments identify vulnerabilities resulting from non-safety-related equipment, additional structures, systems, and components should be considered for inclusion within this definition.

Mitigated event: As used in this standard, a mitigated event involves the following sequence:

- An initiating event that could lead to a release from the primary confinement barrier
- Failure of all elements of the control strategy that would prevent the initiating event from developing into a release from the primary confinement barrier
- Mitigation of the consequences of the release as provided by the control strategy

Mitigated event frequency: The mitigated event frequency is the corresponding release frequency times the probability that the elements of the control strategy that mitigate the release will function given the release.

Release frequency: The release frequency is the product of the frequency of the initiating event times the probability that all elements of the control strategy that would prevent the release fail, given the initiating event.

Reliability: The probability that an SSC will perform its safety function when required.

Unmitigated event: As used in this standard, an unmitigated event involves the following sequence:

- An initiating event that could lead to a release from the primary confinement barrier
- Failure of all elements of the control strategy that would prevent the initiating event from developing into a release from the primary confinement barrier
- Failure of all elements of the control strategy that would mitigate the consequences of the release

Unmitigated event frequency: The frequency of an unmitigated event is the corresponding release frequency times the probability that all elements of the control strategy that would mitigate the release fail, given the release.